REMARKS

In view of the following remarks, Applicant respectfully requests reconsideration of the present application.

Objections and Rejections

The Office Action dated August 25, 2004:

1. objects to the abstract of the disclosure because of undue length;
2. rejects claims 40 and 41 under 35 U.S.C. § 102(b) as being anticipated by United States Patent no. 5,581,616 entitled "Method and Apparatus for Digital Signature Verification" that issued December 3, 1996, on a patent application filed by Richard E. Crandall ("the Crandall '616 patent");
3. rejects claims 1-5, 12-18, 25-31, 38 and 39 under 35 U.S.C. § 103(a) as being unpatentable over:
   a. United States Patent no. 4,200,770 entitled "Cryptographic Apparatus and Method" that issued April 28, 1980, on a patent application filed by Martin E. Hellman, Bailey W. Diffie and Ralph C. Merkle ("the Hellman, et al. patent"); in view of
   b. "Applied Cryptography" © 1996 by Bruce Schneier, published by John Wiley & Sons, Inc. ("Schneier");

4. rejects claims 6-11, 19-24 and 32-37 under 35 U.S.C. § 103(a) as being unpatentable over:
   a. the Hellman, et al. patent;
   b. in view of Schneier; and further in view of
   c. United States Patent no. 5,159,632 entitled "Method and Apparatus for Public Key Exchange in a Cryptographic System" that issued October 27, 1992, on an application filed by Richard E. Crandall ("the Crandall '632 patent").

Abstract Complies With 37 C.F.R. § 1.72

For the following reason, Applicant respectfully requests withdrawal of the undue length objection to the Abstract.

Attached hereto as Exhibit A is a copy of the patent application's abstract as originally filed annotated along the right hand edge with the number of words in the line of text extending leftward from each annotation. The sum formed by adding together all the numbers annotated along the right hand edge of Exhibit A is 150. Since as demonstrated by Exhibit A the Abstract does not exceed 150 words, Applicant respectfully:

1. submits that the Abstract as originally filed fully complies with 37 C.F.R. § 1.72; and

2. therefore, requests that the objection thereto appearing in the August 25, 2004 Office Action be withdrawn.

The Claimed Invention

The invention, as embodied in **independent claim 40**, is a three (3) step method by which a receiving unit R that receives a message M and a digital signature authenticates the digital signature.

1. Step 1 requires **retrieving a plurality of public quantities from a publicly accessible repository**.
2. Step 2 requires **evaluating expressions of at least two (2) different verification relationships** using:
   a. **the received digital signature**; and
   b. **the plurality of public quantities**;
3. Step 3 requires **comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships**.

The invention, as embodied in **independent claim 27**, is **a cryptographic unit** that includes:

1. **ports**; and
2. **a cryptographic device**.

When **the cryptographic unit** encompassed by independent claim 27 **is to receive a cyphertext message M**, the **ports**:

1. **store a plurality of public quantities in a publicly accessible repository**; and
2. **receive** via the communication channel I **a plurality of sender's quantities from a sending cryptographic unit**.

The receiving cryptographic unit uses the plurality of sender's quantities and at least some of the plurality of public quantities in **computing**:

1. **at least one receiver's quantity** which said receiving cryptographic unit transmits via the communication channel I to said sending cryptographic unit; and
2. a cryptographic key K.

When **the cryptographic unit** encompassed by independent claim 27 is **to send the cyphertext message M**, the **ports retrieve the plurality of public quantities from the publicly accessible repository**. The **sending cryptographic unit** then uses the retrieved plurality of public quantities in **computing**:

1. **the plurality of sender's quantities** which the sending cryptographic unit transmits via the communication channel I to the receiving cryptographic unit; and
2. after receiving via the communication channel I the receiver's quantity from the receiving cryptographic unit, **the cryptographic key K**.

In addition to the ports, **the cryptographic unit** encompassed by independent claim 27 also includes **a cryptographic device**. **The cryptographic device** includes:

1. **a key input port**;
2. **a plaintext port**; and
3. **a cyphertext port**.

The key input port receives the cryptographic key K. The plaintext port:

1. accepts a plaintext message P for encryption into the cyphertext message M; and
2. delivers a plaintext message P obtained by decrypting a received cyphertext message M.

The cyphertext port, which is coupled to one a transceiver included in a cryptographic system:

1. transmits the cyphertext message M to the transceiver; and
2. receives the cyphertext message M from the transceiver.

The Cited References

The Crandall '616 Patent

The Crandall '616 patent discloses a method and apparatus that:

> improves speed and reduces complexity in a digital signature scheme that uses elliptic algebra. **The signa-**

> **ture scheme generates two points that are compared. If the points do not match, the signature is not authentic.** (Abstract) (Emphasis supplied.)

Regarding transmitting a plurality of public quantities for storage in a publicly accessible repository as expressly recited in the preamble of independent claim 40, **in rejecting that claim the August 25, 2004, Office Action identifies**:

1. **FIGs. 8-12, especially FIG. 12,** in the Crandall '616 patent; and

2. the following **text** which appears **in column 1 at lines 50-56** in that reference.

> Such a function is referred to as a "one way function" or as a "trap door function." **In a public key cryptosystem, certain information relating to the keys is public. This information can be, and often is, published or transmitted in a non-secure manner.** Also, certain information relating to the keys is private. This information may be distributed over a secure channel to protect its privacy, (or may be created by a local user to ensure privacy). (Emphasis supplied.)

While the preceding text excerpted from the Crandall '616 patent clearly discloses the publication or transmission of public keys in a non-secure manner, it fails to disclose or to suggest a "sending unit S" transmitting "for storage in a publicly accessible repository **a plurality of public quantities**" as expressly required by the preamble text of independent claim 40. Therefore, **if the Crandall '616 patent is to anticipate this particular aspect which**

appears in the preamble of pending independent claim 40, then the Crandall '616 patent's disclosure must reside either:

1. in FIG. 12; or
2. in the text of the Crandall '616 patent describing FIG. 12.

The text of the Crandall '616 patent describes FIG. 12 as "a block diagram for implementing the digital signature scheme of the present invention." In FIG. 12, the Crandall '616 patent depicts a "public source 813." Regarding the "public source 813," the text of the Crandall '616 patent beginning in column 19 at line 34 and continuing to column 20 at line 37 further discloses that:

> The **encryption/decryption means 1204 of receiver 1202** is coupled to elliptic multiplier 806 through line 810. The elliptic multiplier 806 is coupled to the private key source 808 through line 812. The point u is provided to the elliptic multiplier 806 from the nonsecure channel 816 via line 1212. Elliptic multiplier 806 generates point Q and provides it to comparator 1208 via line 1216. **Hasher 1206 recieves the ciphertext message C and point P from nonsecure channel 816 via line 1210, and ourPub from source 813 via line 1218**. Hasher 1206 outputs point R to comparator 1208 via line 1214.
>
> *　　　　　　*　　　　　　*
>
> A separate **source 813** stores publicly known information, such as the public keys "ourPub"and "theirPub" of sender 1201 and receiver 1202, the initial point (x_1, y_1), the field F_{pk}, and curve parameter "a". This source of information may be a published directory, an on-line source for use by computer systems, or it may transmitted between sender and receiver over a non-secure transmission medium. The public source 813 is shown symbolically connected to sender 1201 through line 815 and to receiver 1202 and hasher 1206 through lines 814 and 1218 respectively.
>
> *　　　　　　*　　　　　　*

> The elliptic multiplier 806 of the receiver 1202 receives point u from the nonsecure channel 816. The elliptic multiplier 806 generates point Q and provides it to comparator 1208. **Hasher recieves the ciphertext message C and point P from the nonsecure channel 816 and the purported senders public key ourPub from source 813 and generates point R, which it provides to comparator 1208**. **Comparator 1208 compares points Q and R and if they match, the signature is assumed to be valid**. (Emphasis supplied.)

The preceding texts excerpted from the Crandall '616 patent clearly establishes that **a hasher 1206** included in the encryption/decryption means 1204 of **receiver 1202 receives a single value, "ourPub," from the public source 813** via line 1218. However, **with regard to the express text appearing in the preamble of pending claim 40, the arrows appearing in FIGs. 8 and 12 both fail to indicate that the sending unit 1201 "transmits for storage in a publicly accessible repository, such as the public source 813, a plurality of public quantities**."

With regard to storage of public quantities into the "public source 813," beginning in column 7 at line 58 and continuing to column 8 at line 16 the Crandall '616 patent discloses:

> [i]t is necessary that both sender and recipient use the same set of such parameters. Both sender and recipient generate a mutual one-time pad, **as a particular x-coordinate on the elliptic curve**.
>
> In the following description, **the terms "our" and "our end" refer to the sender**. **The terms "their" and "their end" refer to the receiver**. This convention is used because the key exchange of the present invention may be accomplished between one or more senders and one or more receivers. Thus, "our" and "our end" and "their" and "their end" refers to one or more senders and

> receivers, respectively. The public key exchange of the elliptic curve cryptosystem of the present invention is illustrated in the flow diagram of FIG. 3.
>
> Step 301
> At our end, **a public key is computed: ourPub** ϵ F_{pk}
>
> ourPub = (ourPri)$^\circ$(x_1, y_1) Equation (12)
>
> Step 302
> At their end, **a public key is computed: theirPub** ϵ F_{pk}
>
> theirPub = (theirPri)$^\circ$(x_1, y_1) Equation (13)
>
> Step 303
> **The two public keys ourPub and theirPub are published, and therefore known to all users**. (Emphasis supplied.)

Concerning the preamble of independent claim 40, the preceding excerpt from the Crandall '616 patent discloses that:

1. **the sender computes a single quantity, ourPub, a particular x-coordinate on the elliptic curve**; and
2. publishes ourPub, apparently by storing it into the public source 813.

A disclosure of digital signature generation appears in column 16 at lines 22-41 the Crandall '616 patent.

> Assume a curve parameterized by a, with starting point (X_1/1). The sender's public key ourPub is generated as the multiple ourPri$^\circ$(x_1/1), where ourPri is our private key (an integer) and $^\circ$ is multiplication on the elliptic curve. The digital signature is created as follows:
> 1) Choose a random integer m of approximately q bits.
> 2) Compute the point
>
> P = m$^\circ$(X_1/1).

> 3) Using a message digest function M, compute the integer
>
> $$u = m + our\ Pri*M(ciphertext,\ P)$$
>
> where ciphertext is the encrypted message to be sent.
>
> 4) Along with the ciphertext, transmit **the digital signature as the pair (u, P)**. Note that **u is an integer of about 2^q bits, while P is a point on the curve**.

The preceding excerpt from the Crandall '616 patent establishes that **the digital signature**, which is transmitted together with the cyphertext C, **is a pair (u, P) in which u is an integer of about 2^q bits, while P is a point on the elliptic curve.**

The preceding texts excerpted from the Crandall '616 patent establish that **for digital signature authentication, in addition to the Hasher 1206 computing the quantity R, the elliptic multiplier 806 must compute the quantity Q**. Regarding the quantity Q the Crandall '616 patent in column 16 at lines 48 through 62 discloses that:

> [t]he receiver attempts to authenticate the signature by generating a pair of points to match the digital signature pair, using the ciphertext message and the public key of the purported sender. The receiver verifies the signature using the following steps:
>
> 1) **Using the u part of the signature, compute the point**
>
> $$Q = u^\circ(X_1 /1)$$
>
> 2) **Compare the point Q to the point**
>
> $$R = P + M(ciphertext,\ P)^\circ ourPub$$

> **The signature is invalid if these elliptic points Q and R do not compare exactly.**

The Hellman, et al. Patent

The Hellman, et al. patent discloses a:

> cryptographic system transmits a computationally secure cryptogram over an insecure communication channel without prearrangement of a cipher key. A secure cipher key is generated by the conversers from transformations of exchanged transformed signals. The conversers each possess a secret signal and exchange an initial transformation of the secret signal with the other converser. The received transformation of the other converser's secret signal is again transformed with the receiving converser's secret signal to generate a secure cipher key. (Abstract)

For generating a cipher key, the Hellman, et al. patent discloses that:

> a first converser transforms, in a manner infeasible to invert, a first signal while a second converser transforms, also in a manner infeasible to invert, a second signal. The first converser transmits the transformed first signal to the second converser, keeping the first signal secret, and the second converser transmits the transformed second signal to the first converser, keeping the second signal secret. The first converser then transforms the first signal with the transformed second signal to generate a third signal, representing a secure cipher key, that is infeasible to generate solely by transforming the transformed first signal and the transformed second signal. And, the second converser transforms the second signal with the transformed first signal to generate a fourth signal, also representing the secure cipher key, that is infeasible to generate solely by transforming the transformed first signal and the transformed second signal. (Col. 2, lines 35-52.)

For a specific embodiment of invention described in the preceding excerpt from the Hellman, et al. patent, that reference discloses in column 4 at lines 1 through 51 that:

> [c]onverser 11 and converser 12 include independent key sources 25 and 26 respectively, which generate numbers or signals that represent numbers.
>
> *   *   *
>
> Key source 25 generates three signals, q, a, and X_1, and key source 26 generates X_2; . . . . Signals q and a are transmitted to the secure key generator 21 and are transmitted through the insecure channel 19 to secure key generator 22. Signals X_1 and X_2 are kept secret by converser 11 and converser 12 respectively, are given to the secure key generators 21 and 22 respectively, but are not transmitted through the insecure channel 19.
>
> Converser 11 and converser 12 also include secure key generators 21 and 22 respectively, which accept the signals generated by the respective key sources 25 and 26. Secure key generator 22 also receives the signals q and a which are transmitted through the insecure channel 19. The secure key generators 21 and 22 generate signals Y_1 and Y_2 respectively by transforming X_1 and X_2 respectively with signals q and a in a manner that is easily performed but extremely difficult or infeasible to invert.
>
> *   *   *
>
> Signal Y_1 may be generated to represent the number obtained by raising the number represented by signal a to the power represented by signal X_1, modulo the number represented by signal q; this transformation may be represented symbolically as $Y_1 = a^{X_1} \bmod q$. Signal Y_2 may be generated to represent the number obtained by raising the number represented by signal a to the power represented by signal X_2, modulo the number represented by signal q; this transformation may be represented symbolically as $Y_2 = a^{X_2} \bmod q$.
>
> Signals Y_1 and Y_2 are exchanged by transmitting Y_1 and Y_2 through the insecure channel 19 to secure key generators 22 and 21 respectively. Secure key generator 21 then generates a secure key K by transforming signal Y_2 with signals q, a and X_1, and secure key generator 22 generates the same secure key K by transforming Y_1 with signals q, a and X_2.

The Hellman, et al. patent further discloses in column 8 at lines 21 and 22 that the "signals q and a may be public knowledge rather than generated by the key source 25." That is, the Hellman, et al. patent implicitly discloses that the converser 11, which generates the signals q and a, might place them in a publicly accessible repository.

For an example of cipher key generation which is more specific to the text of pending independent claim 27, choose the converser 11 disclosed in the Hellman, et al. patent to be the receiver and the converser 12 to be the sender. If the receiving converser 11 were to make the signals q and a public knowledge, e.g. by storing them into a publicly accessible repository, then to obtain a secure decrypting cipher key K receiving converser 11 transforms Y_2, received from sending converser 12, with public signals q and a together with the receiving converser 11's secret signal X_1. Moreover, the receiving converser 11 also transforms its secret signal X_1 using the signals q and a to obtain Y_1 which it transmits to the sending converser 12.

Continuing with the example of cipher key generation which is more specific to the text of pending independent claim 27 in which the converser 11 disclosed in the Hellman, et al. patent is the receiver and the converser 12 is the sender, to obtain a secure encrypting cipher key K sending converser 12 transforms Y_1, received from receiving converser 11, with public signals q and a together with the sending converser 12's secret signal X_2. Moreover, the sending converser 12 also transforms its secret signal X_2 using the signals q and a to obtain Y_2 which it transmits to the receiving converser 11.

Legal Principles Applicable to Rejections Under 35 U.S.C. 102(b)

> [F]or anticipation under 35 U.S.C. § 102, the reference must teach **every aspect** of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. Manual of Patent Examining Procedure ("MPEP") Eighth Edition Revision 2, May 2004, § 706.02, p. 700-21 (Emphasis supplied)

"Anticipation under 35 U.S.C. § 102 requires the disclosure in a single piece of prior art of each and every limitation of a claimed invention." Rockwell International Corporation v. The United States, 147 F.3d 1358, 1363, 47 USPQ2d 1027, 1031 (Fed. Cir. 1998) citing National Presto Indus. v. West Bend Co., 76 F.3d 1184, 1189, 37 USPQ2d 1685, 1687 (Fed. Cir. 1966).

Argument

Applicant respectfully submits that for the reasons specifically set forth in detail below independent claims 40 and 27 traverse all bases for rejection appearing in the Office Action dated August 25, 2004. Furthermore, because independent claim 27 traverses all bases for rejection, independent claims 1 and 14 similarly traverse rejection. Finally, because claims 2-13, 15-26, 28-39 and 41 respectively depend from independent claims 1, 14, 27 and 40, and because those independent claims traverse rejection, dependent claims 2-13, 15-26, 28-39 and 41 also traverse any and all rejections appearing in the August 25, 2004, Office Action.

Claim 40 Traverses Rejection

Independent claim 40 has been rejected under 35 U.S.C. § 102(b) based upon the Crandall '616 patent. With regard to FIG. 12, the Crandall '616 patent clearly discloses that:

> [a] sender, represented by the components within dashed line 1201, encrypts a plaintext message Ptxt to a ciphertext message C and generates a signature (u, P). This message C and signature (u, P) is sent to a receiver, represented by the components within dashed line 1202. **The receiver 1202** decrypts the ciphertext message C to recover the plaintext message, and **authenticates the signature (u, P)**. (Col. 19, lines 14-20.) (Emphasis supplied.)

However, as best summarized in the table attached hereto as Exhibit B and as explained in greater detail above, with respect to the text of independent claim 40 the Crandall '616 fails to disclose or to suggest:

1. that the "sender 1201" stores **a plurality of public quantities** into the "public source 813" which the

"receiver 1202" retrieves during digital signature authentication;

2. at least **two (2) expressions are evaluated** by the receiver **using a plurality of public quantities**; and

3. comparing **the at least two (2) expressions evaluated using a plurality of public quantities**.

Rather, for digital signature authentication the Crandall '616 patent expressly discloses that:

1. the **"sender 1201" stores a single x-coordinate**, ourPub, into the "public source 813" rather than a plurality of quantities;

2. the "receiver 1202" **evaluates** with the "hasher 1206" an expression to obtain **the quantity R using the single x-coordinate**, ourPub, received from the "public source 813;"

3. the "receiver 1202" **evaluates** with the "elliptic multiplier 806" an expression to obtain **the quantity Q without using any quantity received from the "public source 813**;" and

4. **authenticates** the digital signature **by comparing**:

   a. **the quantity R evaluated using the single x-coordinate public quantity**, ourPub, received from the "public source 813;" and

b. **the quantity Q evaluated without using any quantity received from the "public source 813."**

For the preceding reasons, there exists several essential differences between the disclosure of the Crandall '616 patent and the invention encompassed by pending independent claim 40. Therefore, because the Crandall '616 patent fails to disclose each and every limitation expressly required by the text of pending independent claim 40, Applicant respectfully:

1. submits that independent claim 40 traverses rejection under 35 U.S.C. § 102(b) based upon the Crandall '616 patent; and
2. requests that the rejection of independent claim 40 appearing in the August 25, 2004, Office Action be withdrawn.

Claim 27 Traverses Rejection

Applicant acknowledges that the Hellman, et al. patent discloses everything recited in the preamble of independent claim 27, and everything recited in element "b. a cryptographic device" in the body of that claim. Applicant further acknowledges that the Hellman, et al. patent implicitly discloses in column 8 at lines 21 and 22 storing a plurality of public quantities, i.e. the signals q and a, in a publicly addressible repository. However, Applicant respectfully submits that the Hellman, et al. patent fails to disclose or to suggest either sub-element "i" or sub-element "ii" of element "b. ports" in the body of independent claim 27.

Regarding sub-element "ii" of element "b. ports" in the body of independent claim 27, presume that converser 11 depicted in FIG. 1 of the Hellman, et al. patent were to make the signals q and a public knowledge as expressly disclosed in column 8 at lines 21 and 22, for example by storing them in a publicly accessible repository as required by the text of independent claim 27. Then, if converser 12 were to be the sender of the cyphertext message M as recited in the text of claim 27, in accordance with the disclosure of the Hellman, et al. patent in column 4 at lines at lines 1 through 51 sending converser 12 obtains its encrypting cipher key K by transforming Y_1, received from receiving converser 11, with the public signals q and a together with sending converser 12's secret signal X_2. The preceding procedure disclosed in the Hellman, et al. patent for the sending converser 12's obtaining its encrypting cipher key K is the same as that encompassed by sub-element "ii" of element "b. ports" in the body of independent claim 27.

However, sub-element "ii" of element "b. ports" in the body of independent claim 27 also requires that sending converser 12 use the retrieved plurality of public quantities, i.e. q and a, in computing a plurality of sender's quantities which the sending converser 12 send to the receiving converser 11. With regard to this aspect of sub-element "ii" of element "b. ports," the Hellman, et al. patent discloses that **the sending converser 12**:

1. **first generates Y_2** by transforming sending converser 12's secure signal X_1 with the public quantities, i.e. q and a; and
2. **then transmits only Y_2 to the receiving converser 11**.

Contrasted with the preceding disclosure from the Hellman, et al. patent, **sub-element "ii" of element "b. ports" in independent claim 27 requires** that the "sending cryptographic unit" transmit **a plurality of "sender's quantities"** to the "receiving cryptographic unit." Since the Hellman, et al. patent discloses that **the sending converser 12 transmits only a single quantity Y_2 to the receiving converser 11**, and since **that reference fails to suggest that the sending converser 12 transmit anything in addition to the single quantity Y_2 to the receiving converser 11**, Applicant respectfully submits that the Hellman, et al. patent does not disclose nor does the reference suggest sub-element "ii" of element "b. ports" of pending independent claim 27.[1]

[1] The mathematical operations disclosed in column 8 of the Hellman, et al. patent as being performed by the conversers 11 and 12 use everything disclosed there. After the sending converser 12 transmits Y_2 to the receiving converser 11, **the mathematical operations which**

Regarding sub-element "i" of element "b. ports" in the body of independent claim 27, continue presuming that converser 11 depicted in FIG. 1 of the Hellman, et al. patent makes the signals q and a public knowledge storing them in a publicly accessible repository as required by the text of independent claim 27. Also continue considering the converser 11 disclosed in the Hellman, et al. patent as the receiver of the cyphertext message M transmitted by sending converser 12. In accordance with the disclosure of the Hellman, et al. patent in column 4 at lines at lines 1 through 51 receiving converser 11 obtains its decrypting cipher key K by transforming Y_2, received from sending converser 12, with the public signals q and a together with receiving converser 11's secret signal X_1. Contrasted with the preceding disclosure from the Hellman, et al. patent, **sub-element "i" of element "b. ports" in independent claim 27 requires** that the receiving cryptographic unit use **a plurality of senders quantities** together with some of the plurality of public quantities, e.g. q and a, in computing its decrypting cipher key K. Since the Hellman, et al. patent discloses that **the sending converser 12 transmits only a single**

it performs produce nothing else that could be transmitted to receiving converser 11. Moreover, if sending converser 12 were to transmit something in addition to Y_2, **the mathematical operations performed by the receiving converser 11 have no use the additional item transmitted by sending converser 12**.

quantity Y_2 to the receiving converser 11, and since **that reference fails to suggest that the sending converser 12 transmit anything in addition to the single quantity Y_2 to the receiving converser 11**, Applicant respectfully submits that for this **first** reason the Hellman, et al. patent does not disclose nor does the reference suggest sub-element "i" of element "b. ports" of pending independent claim 27.[2]

Furthermore, sub-element "i" of element "b. ports" in the body of independent claim 27 also requires that **receiving converser 11 use at least some of the retrieved plurality of public quantities**, e.g. q and a, **together with a plurality of senders quantities** in computing at least one receiver's quantity, e.g. Y_1, which the receiving converser 11 sends to the sending converser 12. **Since** as explained above in connection with sub-element "ii" of element "b. ports" **the sending converser 12 sends only a single quantity Y_2 to the receiving converser 11, it is impossible for the receiving converser 11 to use a plurality of senders quantities in computing**

[2] The mathematical operations disclosed in column 8 of the Hellman, et al. patent as being performed by the conversers 11 and 12 use everything disclosed there. After the sending converser 12 transmits Y_2 to the receiving converser 11, **the mathematical operations which it performs produce nothing else that could be transmitted to receiving converser 11**. Moreover, if sending converser 12 were to transmit something in addition to Y_2, **the mathematical operations performed by the receiving converser 11 have no use the additional item transmitted by sending converser 12**.

the at least one receiver's quantity, e.g. Y_1. For this second reason the Hellman, et al. patent does not disclose nor does the reference suggest sub-element "i" of element "b. ports" of pending independent claim 27.

The August 25, 2004, Office Action rejects independent claim 27 under 35 U.S.C. § 103(a) based upon the Hellman, et al. patent in view of Schneier. Paragraph no. 12 of the August 25, 2004, Office Action explains the pertinence of Schneier as follows.

> Hellman does not expressly disclose storing a plurality of public quantities in a publicly accessible repository. However, the variables q and a used in Diffie-Hellman key exchange are public variables within a public-key cryptosystem, which enables these public variables to be published in a public repository as taught by Schneier. See Schneier, page 32, 2nd paragraph; page 515, 'Key Exchange Without Exchanging Keys'. Furthermore, a third party repository acts as a disinterested member of a communications system and can ensure the certification, renewal and cancellation of public information. See Schneier, page 23, 'Arbitrated Protocols'. It would be obvious to one of ordinary skill in the art at the time the invention was made to store the plurality of public quantities in a public accessible repository and retrieve the plurality of public quantities from the public accessible repository for secure key exchange to simplify the key exchange process. See Schneier, page 32, 3rd paragraph. The aforementioned covers claim 27.

Applicant notes that while the Hellman, et al. patent may not "expressly disclose storing a plurality of public quantities in a publicly accessible repository" as stated in the preceding excerpt from the August 25, 2004, Office Action, **Applicant respectfully submits that lines 21 and 22 in column 8 of the Hellman, et al.**

patent implicitly and necessarily make such a disclosure. The text in lines 21 and 22 in column 8 of the Hellman, et al. patent states that:

> signals q and a may be public knowledge rather than generated by the key source 25.

While the preceding excerpt from the Hellman, et al. patent doesn't expressly mention a publicly accessible repository, for q and a to be publicly known the only alternative to them being available in a publicly accessible repository is for them to be part of each individual's instinct at birth. Since the latter alternative appears highly unlikely if not impossible, it appears that making q and a "public knowledge" necessarily requires that they be made available in some sort of publicly accessible repository.

Because, for the preceding reasons the Hellman, et al. patent implicitly discloses "storing a plurality of public quantities in a publicly accessible repository," Applicant respectfully submits that **Schneier** as applied to claim pending in the present application by paragraph 12 **adds nothing to the disclosure of the Hellman, et al. patent**. Since Schneier as applied to claim pending in the present application by paragraph 12 adds nothing to the disclosure of the Hellman, et al. patent, and since for the reasons set forth above the Hellman, et al. patent fails to disclose or to suggest either sub-element i. or ii. of element b. in independent claim 27, Applicant respectfully:

1. submits that independent claim 27 traverses rejection under 35 U.S.C. § 103(a) based upon the Hellman, et al. patent in view of Schneier; and
2. requests that the rejection of independent claim 27 appearing in the August 25, 2004, Office Action be withdrawn.

Independent Claims 1 & 14 Traverse Rejection

Applicant agrees respectively with paragraphs 18 and 19 in the August 25, 2004, Office Action that:

1. independent claim 1 is a method claim corresponding to independent claim 27; and
2. independent claim 14 is a system claim corresponding to independent claim 27.

Therefore, because for the reasons set forth above independent claim 27 traverses rejection under 35 U.S.C. § 103(a) based upon the Hellman, et al. patent in view of Schneier, Applicant respectfully submits that independent claims 1 and 14 also traverse rejection based upon that combination of references.

Dependent Claims 2-13, 15-26, 28-39 and 41 All Traverse Rejection

Dependent claims 2-13, 15-26, 28-39 and 41 respectively depend from independent claims 1, 14, 27 and 40. Because for the reasons set forth above independent claims 1, 14, 27 and 40 traverse rejection on the bases set forth in the August 25, 2004, Office Action, Applicant respectfully submits that claims 2-13, 15-26, 28-39 and 41, which depend respectively from independent claims 1, 14, 27 and 40, also traverse rejection for any and all reasons appearing in the August 25, 2004, Office Action.

Conclusion

Because, as demonstrated by Exhibit A attached hereto the abstract as original filed contains only 150 words, Applicant respectfully requests that the objection thereto be withdrawn.

Because for the reasons set forth above independent claim 40 traverses rejection under 35 U.S.C. § 102(b) based upon the Crandall '616 patent, Applicant respectfully requests:

1. that the rejection of independent claim 40 together with the rejection of claim 41 depending therefrom based upon the Crandall '616 patent be withdrawn; and
2. that claims 40 and 41 pass promptly to issue.

Because for the reasons set forth above independent claim 27 traverses rejection under 35 U.S.C. § 103(a) based upon the Hellman, et al. patent in view of Schneier, Applicant respectfully requests:

1. that the rejection of independent claim 27 together with any and all rejections of claim 28-39 depending therefrom based upon that combination of references, either alone or in further combination with any other reference(s), be withdrawn; and
2. that claims 27 through 30 pass promptly to issue.

Because for the reasons set forth above independent claim 1 traverses rejection under 35 U.S.C. § 103(a) based upon the Hellman, et al. patent in view of Schneier, Applicant respectfully requests:

1. that the rejection of independent claim 1 together with any and all rejections of claim 2-13 depending therefrom based upon that combination of references, either alone or further in combination with any other reference(s), be withdrawn; and
2. that claims 1 through 13 pass promptly to issue.

Because for the reasons set forth above independent claim 14 traverses rejection under 35 U.S.C. § 103(a) based upon the Hellman, et al. patent in view of Schneier, Applicant respectfully requests:

1. that the rejection of independent claim 14 together with any and all rejections of claim 15-26 depending therefrom based upon that combination of references, either alone

or further in combination with any other reference(s), be withdrawn; and

2. that claims 14 through 26 pass promptly to issue.

For the preceding reasons, the Applicant respectfully requests favorable reconsideration and allowance of claims 1-41 presently pending in this application.

Respectfully submitted,

Donald E Schreiber

Donald E. Schreiber
Reg. No. 29,435

Dated: 25 January, 2004

Donald E. Schreiber
A Professional Corporation
Post Office Box 2926
Kings Beach, CA 96143-2926

Telephone: (530) 546-6041

Attorney for Applicant